Active Directory Privilege Escalation Checklist

- [ ] Kerberos TGS Service Ticket Cracking (Kerberoast)
- [ ] Excessive Amount of Domain Admins
- [ ] Incorrectly Configured Forest or Domain Trust
- [ ] Misconfigured Access Control Lists
- [ ] Password Spraying
- [ ] Passwords in Active Directory Attributes
- [ ] SMB Shares Mining
- [ ] Unsafe Usage of High Privileged Accounts
- [ ] NTLM Relaying and Theft
- [ ] Check for Local Admin Privileges
- [ ] Credential Extraction (LSASS/SAM)
- [ ] Check for Lockout Policy
- [ ] Check for misconfigured LAPS
- [ ] Check for writable executables on shares
- [ ] Abusing GPO
- [ ] ASEP Roasting
- [ ] Misconfigured SQL-server
- [ ] Get Passwords Stored in SYSVOL Group Policy Preference
- [ ] Check for scripts on DC SYSVOL
- [ ] Misconfigured read only domain controller
- [ ] LLMNR and NBT-NS Poisoning